**Summary of the Security Event:**

The security event involved a distributed denial of service (DDoS) attack on the organization's network, which disrupted services for two hours. The attack exploited an unconfigured firewall, flooding the network with ICMP packets and rendering internal services inaccessible.

**Identification:**

Type of Attack: Distributed Denial of Service (DDoS) Systems Impacted: Internal network services, causing disruption to normal operations

**Protection Plan:**

1. Implement Proper Firewall Configuration:
   * Configure firewall rules to limit the rate of incoming ICMP packets.
   * Enforce source IP address verification on the firewall to prevent spoofed IP addresses on incoming ICMP packets.
2. Employee Training and Policies:
   * Provide training to network administrators on best practices for configuring and maintaining firewalls.
   * Establish policies and procedures for network security, including regular audits and vulnerability assessments.

**Detection Methods:**

1. Network Monitoring:
   * Deploy network monitoring software to detect abnormal traffic patterns.
   * Monitor network logs and traffic for signs of anomalous behavior, such as sudden spikes in ICMP traffic.
2. Intrusion Detection and Prevention Systems (IDS/IPS):
   * Utilize IDS/IPS systems to filter out suspicious ICMP traffic based on predefined characteristics.
   * Set up alerts and notifications within IDS/IPS systems to promptly identify and respond to potential threats.

**Response Plan:**

1. Immediate Response:
   * Block incoming ICMP packets to mitigate the attack.
   * Take non-critical network services offline to preserve critical resources.
   * Restore critical network services to minimize downtime.
2. Future Incident Response:
   * Establish an incident response team with clearly defined roles and responsibilities.
   * Develop incident response procedures and communication protocols to facilitate a coordinated response to future incidents.

**Recovery Plans:**

1. Restore Affected Systems:
   * Recover affected systems to normal operation after the incident is contained.
   * Restore data and assets that have been compromised or affected by the incident.
2. Post-Incident Analysis:
   * Conduct a post-incident analysis to identify lessons learned and areas for improvement.
   * Implement necessary changes to enhance the organization's resilience against future cyber threats.